IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Examiner: Jung, David Y.
Takatoshi Ono et al.	Group Art Unit: 2134
Serial No.: 10/763,958	
Filed: January 23, 2004	
For: ELLIPTIC CURVE EXPONENTIATION APPARATUS THAT CAN COUNTER DIFFERENTIAL FAULT ATTACK, AND INFORMATION SECURITY APPARATUS	August 31, 2007 Costa Mesa, California 92626

RESPONSE TO OFFICE ACTION

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Office Action mailed June 4, 2007, please amend the above-identified application as follows:

IN THE CLAIMS

1-9. (Cancelled.)

10. (Currently Amended) An information security apparatus that ensures secure handling of predetermined information by computing an elliptic curve exponentiation of $k*Q$, based on computational complexity of solving a discrete logarithm problem on an elliptic curve $E:y^2=x^3+aXx+b$ defined over a residue field F with a prime p being a modulus, comprising:

an information obtaining unit operable to obtain a point Q that is on the elliptic curve E, and an exponent k that is a positive integer smaller than the prime p;

a first storage unit operable to store therein a coefficient a that is ~~an x~~ a linear term of the elliptic curve E;

a computation unit operable to compute an elliptic curve exponentiation of the exponent k and the point Q using the coefficient a stored in the first storage unit, to obtain an exponentiation-result-point $k*Q$;

a judgment unit operable to judge whether the point Q and the obtained exponentiation-result-point $k*Q$ ~~is on~~ are on the elliptic curve E; and

a prohibition unit operable to prohibit an output of the obtained exponentiation-result-point $k*Q$, when a judgment result of the judging unit is negative; and

a processing unit operable to realize, when the judgment result of a judging unit is affirmative, process of: encryption of a plaintext, decryption of a ciphertext; generation of a signature for a plaintext; signature verification for a plaintext and a signature; or a process of

sharing of a secret key between two parties without revealing the secret key to a third party, with the use of the obtained exponentiation-result-point $k*Q$; and

wherein the information obtaining unit obtains coordinates (Qx, Qy) as the point Q,

the computation unit computes coordinates (Qx', Qy') as the exponentiation-result-point $k*Q$, and

the judgment unit judges whether the point Q and the exponentiation-result-point $k*Q$ are on the same elliptic curve, by judging whether $(Qy^2-Qx^3-aXQx) - (Qy'^2- Qx'^3-aXQx') = 0$.

11-14. (Cancelled)

15. (New) An information security method for use in an information security apparatus that ensures secure handling of predetermined information by computing an elliptic curve exponentiation of k*Q, based on computational complexity of solving a discrete logarithm problem on an elliptic curve E: $y^2=x^3+a\times x+b$ defined over a residue field F with a prime p being a modulus, and that includes an information obtaining unit, a first storage unit storing a coefficient a that is a linear term of the elliptic curve E, a computation unit, a judgment unit, a prohibition unit, and a processing unit, the method comprising:

executing an information obtaining step by the information obtaining unit for obtaining a point Q that is on the elliptic curve E, and an exponent k that is a positive integer smaller than the prime p;

executing a computation step by the computation unit for computing an elliptic curve exponentiation of the exponent k and the point Q using the coefficient a stored in the first storage unit, to obtain an exponentiation-result-point k*Q;

executing a judgment step by a judgment unit for judging whether the point Q and the obtained exponentiation-result-paint k*Q are on the elliptic curve E;

executing a prohibition step by the prohibition unit for prohibiting an output of the obtained exponentiation-result-point k*Q, when a judgment result of the judgment step is negative; and

executing a processing step by the processing unit for realizing, when the judgment result of the judgment step is affirmative, processes of: encryption of a plaintext, decryption of a ciphertext; generation of a signature for a plaintext; signature verification for a plaintext and a signature; or a process of sharing of a secret key between two parties without revealing the secret key to a third party, using the obtained exponentiation-result-point k*Q,

wherein, in the information obtaining step, the information obtaining unit obtains coordinates (Qx, Qy) as the point Q;

in the computation step, the computation unit computes coordinates (Qx', Qy') as the exponentiation-result-point k*Q; and

in the judgment step, the judgment unit judges whether the point Q and the exponentiation-result-point k*Q are on the same elliptic curve, by judging whether $(Qy^2 - Qx^3 - a \times Qx) - (Qy'^2 - Qx'^3 - a \times Qx') = 0$.

16. (New) A computer program which, when executed on a computer, performs each of the steps of the method of Claim 15.

17. (New) The computer program of Claim 16, recorded on a computer-readable recording medium.

REMARKS

Claims 1-14 were pending and stand rejected as allegedly unpatentable over European Patent Application No. EP 1 237 322 to Kaminaga et al. ("Kaminaga"), in view of article entitled "Differential Fault Attacks on Elliptic Curve Cryptosystems" by Biehl et al. ("Biehl"), and further in view of article entitled "Validation of Elliptic Curve Public Keys" by Antipa et al ("Antipa"). Applicant respectfully requests reconsideration and withdrawal of the rejection in view of the amendments made herein and the remarks that follow.

Claim Amendments

Claims 1-9 and 11-14 have been cancelled without prejudice or disclaimer to the subject matter claimed therein.

Claim 10 has been amended by incorporating the recitations of dependent claims 8, 9 and 11, all of which are now cancelled. No new matter has been added.

New claims 15-17 have been added to particularly point out and distinctly claim novel embodiments of the disclosure. Specifically, independent claim 15 is directed to a method for implementing information security. Dependent claims 16 and 17 relate, respectively, to a computer program for executing the method of claim 15 and a recording medium for recording the computer program. Support for the new claims is found throughout the specification, for example, at pages 12-14, Fig. 1 and the originally-filed claims 1 and 12-14

No new matter has been added. Entry of the amendments and reconsideration on the merits are respectfully requested.

Obviousness Rejections

In view of the amendments made herein and the remarks that follow, Applicant respectfully submits that the claims are patentable over Kaminaga in view of Biehl and Antipa.

The claimed embodiments relates to method and apparatus for countering differential fault attack ("DFA") by using elliptic curve differentiation. As described fully at pages 2-4 of the specification, a third party can apply a high current to an IC programmed with the secret key and compromise security. To address these and other deficiencies, the embodiment of independent claim 10, as amended (references numeral to an embodiment shown in the drawings are added for the Examiner's convenience), recites:

> wherein the information obtaining unit [122] obtains coordinates (Qx, Qy) as the point Q, the computation unit [124] computes coordinates (Qx', Qy') as the exponentiation-result-point k*Q, and the judgment unit [127] judges whether the point Q and the exponentiation-result-point k*Q are on the same elliptic curve, by judging whether $(Qy^2-Qx^3-aXQx) - (Qy'^2- Qx'^3-aXQx') = 0$.

Similarly, independent claim 15 recites in pertinent portions:

> wherein, in the information obtaining step, the information obtaining unit [122] obtains coordinates (Qx, Qy) as the point Q; in the computation step, the computation unit [124] computes coordinates (Qx', Qy') as the exponentiation-result-point k*Q; and in the judgment step, the judgment unit [127] judges whether the point Q and the exponentiation-result-point k*Q are on the same elliptic curve, by judging whether $(Qy^2- Qx^3-a\times Qx) - (Qy'^2-Qx'^3-a\times Qx')=0$.

Kaminaga, Biehl and Antipa, taken individually or in combination, fail to disclose or suggest at least these features.

Kaminaga is directed to a fault detection method for cryptographic process of confronting an attack. Referring to Fig. 6, Kaminaga discloses receiving a ciphertext C (step 601), storing the ciphertext on a RAM (step 602), decrypting the cyphertext (step 603), and storing the processing result Z in on a RAM (step 604). At step 605, the processing result Z is encrypted to W and the original plaintext C and W are compared. When the processing result W coincides with the original plaintext C, the plaintext Z is output to the I.O port (step 608). If not, the result is effected (step 607). Kaminaga does not contemplate, much less disclose the above-identified recitations of independent claims 10 and 15.

The reference to Biehl fails to cure this deficiency. Biehl is directed to differential fault attacks on elliptic curve cryptosystems. At section 2 of Biehl (cited by the Examiner), the reference discloses the polynomial equations governing elliptic curves and using random register faults to compute information about the secret key. Biehl neither discloses, nor suggests, the above-identified recitations.

The reference to Antipa also fails to disclose or suggest the above-identified recitations. At portions cited by the Examiner (sections 3 and 4 of Antipa), the reference generally discloses public key validation of an elliptic curve and invalid curve attacks. While section 4 of Antipa generally describes invalid-curve attacks, the Examiner has not pointed out and Applicant cannot determine exactly where Antipa discloses the specific claim language recited above.

For at least these reasons, independent claims 10 and 15 are patentable over the references of record. Dependent claims 16-17 are deemed patentable at least by the virtue of their dependence on an otherwise patentable independent claim. The Examiner's reconsideration and withdrawal of the obviousness rejection are respectfully requested.

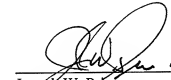
Finally, Applicant also notes that the current amended claims have received an allowance in the European Patent Office over the same art of record. Accordingly, Applicant respectfully requests the Examiner's allowance of the amended claims.

It is submitted that the claims are allowable and an early notice of allowance is solicited.

If the Examiner believes a telephone interview will help further the prosecution of this case, it is respectfully requested he contact the undersigned attorney at the listed phone number.

Very truly yours,

SNELL & WILMER L.L.P.



Joseph W. Price
Registration No. 25,124
600 Anton Boulevard, Suite 1400
Costa Mesa, California 92626-7689
Telephone: (714) 427-7420
Facsimile: (714) 427-7799